U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

PUBLIC RELEASE

OFFICE OF THE SECRETARY

Independent Evaluation of the Department's Information Security Program Under the Government Information Security Reform Act

Executive Summary

Inspection Report No. OSE-14384-01-0001/September 2001

Office of Systems Evaluation

EXECUTIVE SUMMARY

This report presents the Office of Inspector General's independent evaluation of the information security program of the Department of Commerce as required by the Government Information Security Reform Act.[1] The report's structure and content are designed to be responsive to the guidance provided by the Office of Management and Budget. The objective of our evaluation was to determine whether the Department's information security program and practices comply with the requirements of the act, which seeks to ensure proper management and security for the information resources supporting federal operations and assets.

Programs Reviewed and Methodology

Our evaluation is based on the collective results of OIG reviews and audits of (1) the Department's information security program functions assigned to the CIO, (2) the Department's implementation of the Critical Infrastructure Protection Program, (3) general controls associated with the information technology (IT) processing environment at various operating units conducted as part of OIG's fiscal year 2000 financial statements audits,[2] (4) security of the Census Bureau's Advance Retail Sales principal federal economic indicator, and (5) the use of persistent Internet cookies and web bugs on departmental Internet sites.

In order to determine how the agency integrates security into its capital planning and investment control process, we reviewed the capital asset plans and related budget request for fiscal year 2002 and the capital asset plans for fiscal year 2003. In order to determine the specific methods used by the Department to ensure that contractor-provided services are adequately secure, we reviewed a random sample of 40 contract actions for IT services from a universe of awards made by the Department during the period September 1998 through July 2001.

The general control reviews of financial systems and their related networks were conducted using GAO's *Federal Information System Controls Audit Manual* (FISCAM) as a guide and included penetration testing. The other evaluations were conducted using applicable federal laws and policies, as well as Department policies, as criteria.

Our evaluation also includes the results of reviews performed by other parties, which in accordance with OMB guidance, we determined were of sufficient quality, applicability, and independence. In particular, we used the results of the recent evaluation of information security

[1]Title X, subtitle G of the 2001 Defense Authorization Act (P.L. 106-398).

[2]Operating units reviewed were Bureau of the Census, Economic Development Administration, International Trade Administration, National Institute of Standards and Technology, National Oceanic and Atmospheric Administration, National Technical Information Service, and United States Patent and Trademark Office.

in seven Commerce organizations,[3] conducted by the General Accounting Office (GAO), which included penetration testing of systems and networks based in the Herbert C. Hoover Building. We also used results of selected security assessments contracted for by individual operating units, namely, the Census Bureau, the Bureau of Economic Analysis, and the International Trade Administration.

In attempting to reconcile any differences between the OIG's independent evaluation and the Department's program review, it is important to note that because all of our work must be performed in accordance with established audit and inspection standards, some of our data cannot be as current as the data reported by the Department. The Department's review, which was still ongoing as of early September, is based largely on operating unit self assessments provided to the Department in August and September. It is impossible for us to validate the self assessment results in the available time frame, and not all of the information pertaining to the security condition of the operating units, as reported in the Department's review, is consistent with our own findings. Regardless of the differences, we believe that our findings are an accurate reflection of the basic status and issues of the Department's information security program.

We did not include an audit of the evaluation of classified systems as required by the act because such an evaluation has not been conducted and therefore was not available from the Department. We plan to address these systems in next year's report. We are currently evaluating the information security program functions of the Deputy Assistant Secretary for Security that are associated with classified systems and will provide our findings in next year's report, as well.

New Department Emphasis on Information Security to Address Pervasive Weaknesses

Information security weaknesses throughout Commerce have prompted us to identify information security as one of the Department's top 10 management challenges. In addition to our own observations, GAO's recently completed penetration testing of the Commerce headquarters building revealed pervasive computer security weaknesses that place sensitive Commerce systems at serious risk.

Recognizing the severity of this issue, the Department is making a concerted effort to improve information security. In July 2001, the Secretary directed secretarial officers and operating unit heads to give information security high priority, sufficient resources, and their personal attention. The Secretary's IT management restructuring, which recently took effect, is designed to increase the authority and effectiveness of the Department and operating unit CIOs. An IT security task

[3]The Commerce organizations reviewed by GAO were the Office of the Secretary, the Bureau of Export Administration, the Economic Development Administration, the Economics and Statistics Administration, the International Trade Administration, the Minority Business Development Agency, and the National Telecommunications and Information Administration.

force was recently formed, under the direction of the Deputy Secretary, to develop a comprehensive information security program plan for the Department.

Another step toward strengthening information security occurred in June 2001, when the Office of the CIO, the Office of Security, and the OIG, entered into a memorandum of agreement to define their respective roles and responsibilities relating to the development, implementation, and management of the Commerce information security program. This agreement is intended to promote a partnership among the three offices that both ensures complete coverage of information security matters and prevents wasteful duplication of effort.

Evaluation Findings

Our evaluation found that because information security did not receive adequate attention in the past, significant weaknesses exist in policy, implementation, and oversight. Consequently, substantial efforts will be required to develop and oversee an effective information security program. Our findings are summarized below:

- **The Department Needs to Establish a Process to Report Security Deficiencies as Material Weaknesses.** The Security Act requires reporting of significant deficiencies in security policy, procedures, or practices as a material weakness. Circular A-130, *Management of Federal Information Resources*, requires operating units to identify security deficiencies pursuant to Circular A-123, *Management Accountability and Control,* and the Federal Managers' Financial Integrity Act if it is determined that there is no assignment of security responsibility, no security plan, or no accreditation. We found deficiencies associated with these elements throughout the Department that should be evaluated to determine whether they are material weaknesses. The determination to report a material weakness should depend on the risk and magnitude of harm that could result from the weakness. However, the Department lacks a policy or process for reporting information security deficiencies as material weaknesses. The Office of the CIO, along with the operating units, need to immediately identify the most critical departmental systems, define a reporting strategy, and specify milestones.

  Management control weaknesses which, in our opinion, pose a risk or a threat to the internal control systems of an audited entity must be identified and reported, even if the management of the audited entity would not report the weaknesses outside the agency. Our fiscal year 2000 financial statements audits concluded that four operating units had management control weaknesses in system security that rose to the level of "reportable conditions."[4] Taken together, these conditions, combined with the Department's lack of an integrated financial management system, constituted a material weakness in the audit of the consolidated financial statements.

[4]"Reportable conditions"represent significant deficiencies in the design or operation of an internal control.

- **Additional Efforts Are Needed to Improve Risk Assessment, Security Planning, and Test and Evaluation.** The Security Act requires the head of each agency to ensure that appropriate senior agency officials are responsible for assessing the information security risks associated with the operations and assets for programs and systems over which they have control, determining the levels of information security appropriate to protect such operations and assets, and periodically testing and evaluating information security controls and techniques. We found shortcomings in all of these areas.

  Our FISCAM reviews found entitywide security program planning and management needed improvement at all seven locations audited. Likewise, in reviewing 94 sensitive systems in the Department, GAO found that only 3 had documented risk assessments, 1 of which was still in draft and that only 7 had security plans, none of which had been approved by management. GAO also found that none of the systems were accredited.[5] The security assessments contracted for by individual operating units found a lack of documented policies, risk assessments, and security plans, as well as a lack of system accreditations. Operating unit self-assessments conducted in the Summer/Fall 2000 time frame, with oversight by the CIO's office, revealed that for the total population of Commerce IT systems, only 28 percent had risk assessments, 54 percent had security plans, and 8 percent were accredited. Many evaluations also found that information security control techniques are not being periodically tested and evaluated.

  Our Critical Infrastructure Protection (CIP) Program review found that vulnerability assessments have been completed for only 22 of the 241 IT assets deemed to be part of the nation's critical infrastructure, and that plans for determining the controls needed to reduce the vulnerabilities and justify CIP budgets had not been prepared. The CIO's office has noted that these assessments, as well as other required CIP efforts, are part of the overall information security program and that the Department will revise its policy to reflect this approach.

  Finally, our review of the security of the Advance Retail Sales principal economic indicator found issues concerning the designation of positions according to risk and sensitivity.[6] Some employees with advance knowledge of sensitive economic data that could affect or predict financial market activity do not always have the requisite risk classifications or background investigations, and some positions are designated according to national security sensitivity levels rather than the appropriate risk levels, which can

[5]Accreditation is the authorization of a system to process information granted by a management official. By authorizing a system to process information, a manager accepts a certain level of risk associated with it.

[6]Risk classifications address the damage an individual could cause to the efficiency and integrity of government programs and operations, whereas sensitivity classifications address the potential impact on national security.

lead to inappropriate background investigations. These issues exist elsewhere in Commerce and are the result of a lack of current departmental guidance. Therefore, Commerce's program for position designation needs to be updated and strengthened.

- **Additional Efforts Are Needed to Achieve an Adequate Department-wide Security Program, Evaluate Performance, and Ensure Employee Training.** The Security Act gives the CIO responsibility for developing and maintaining an agencywide information security program; ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques; and training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities. We found that substantial improvements are needed in these areas.

  Developed before a major revision of the security requirements of OMB Circular A-130, the Department's information security policy is out of date and needs to be revised and expanded. While the Department's oversight of information security has improved recently, it has performed few information security reviews. As a result, many Commerce systems lack adequate procedures and control techniques, placing information and equipment at risk. Problems include serious, pervasive weaknesses in access controls, inadequate segregation of duties and change control, weak intrusion detection and auditing capabilities, systems running software that is out-of-date or lacks the necessary vendor patches, and inadequate physical security. Moreover, security training is not conducted on a rigorous or ongoing basis, and none of the operating units was able to give us the information we requested on the number of agency employees who received security training or the cost of providing such training. Finally, the Department needs to ensure that the privacy of visitors to its Internet sites is safeguarded by enforcing its policies concerning the use of persistent cookies and web bugs.[7] Toward this end, the Secretary has appointed a senior privacy advisor, who is tasked with ensuring that privacy laws and policies are being followed throughout the Department.

- **Procedures for Detecting, Reporting, and Responding to Security Incidents Should Be Improved.** The Security Act requires agencies to have documented procedures for detecting, reporting, and responding to security incidents. We found that only 4 of 15 operating units have a formal incident response capability, one of which became operational this August, and most operating units have not installed intrusion detection systems. In addition, most operating units have weak or nonexistent auditing capabilities. The lack of auditing, coupled with weak intrusion detection capabilities, make it difficult for operating units to know when a security incident has occurred or who was responsible. In addition, the Department's policy that specifies how information security

[7]Persistent Internet "cookies" are data stored on web users' hard drives that can identify users' computers and track their browsing habits. Web bugs are software code that can monitor who is reading a web page.

incidents should be reported needs to be revised to include reporting to the OIG and to define what constitutes a reportable incident.

Two recent actions should help to address these issues. First, the memorandum of agreement between the CIO's office, OSY, and the OIG specifies that the OIG is to be notified immediately regarding IT system incidents/intrusions, and it defines a process for incident response. Second, the Department has recently begun planning to form a computer incident response team that will cover the operating units that do not have a formal response capability.

- **Capital Asset Plans Should Identify Security Requirements More Explicitly and Link Them to Security Cost Estimates.** For the fiscal year 2002 budget request, OMB began requiring agencies to identify and budget for the security measures and resources that will be needed to protect IT investments, both in the earliest planning stages and throughout the life cycle. Security costs are to be presented in Exhibit 53, "Agency IT Investment Portfolio," and capital asset plans must be provided (Exhibit 300) indicating whether the project's security has met the requirements of the Security Act and describing the security and privacy measures that will be used. We found that while better information on security was presented for fiscal year 2003, the analysis of security requirements, measures, and costs needs improvement. Security was addressed in most fiscal year 2002 capital asset plans, but several plans did not cover this topic, and most did not identify security costs. Security costs were also omitted from the OMB budget request for several projects having capital asset plans. The fiscal year 2003 capital asset plans tend to have more detailed discussions of security, although most still do not identify security costs. Moreover, many of the plans do not clearly identify what the security requirements are or how they will be addressed, and where costs are estimated, they do not describe the basis of the estimate.

- **Refinements Needed to Critical Asset Identification.** The Security Act requires agencies to identify, prioritize, and protect critical assets within their enterprise architecture, including links with key external systems. We found that the reliability of the Department's asset inventory for the CIP program is questionable because of weaknesses in the methodology used to gather asset data, and three of the Department's largest operating units expressed concern that the inventory did not reflect the priority of their assets. To identify the critical asset inventory, the Department planned for operating unit managers to be interviewed by a contractor supporting its CIP program, using a survey questionnaire. However, because of logistical and resource problems in arranging the large number of meetings necessary to complete the questionnaires, operating unit managers with direct responsibility for, and the most knowledge of, the assets generally were not interviewed. In addition, operating units are not considering risks associated with their network interconnections with external systems.

The federal Critical Infrastructure Assurance Office has developed criteria for identifying critical assets that consider how quickly the asset would have to be reconstituted in an emergency. By applying the new criteria, the CIO's office expects the number of assets on the list to be significantly reduced from its current level of 241, allowing it to focus attention on those that are most critical.

- **The Department Needs to Provide Guidance and Develop Procedures To Ensure That Contractor-Provided IT Services are Secure.** The Security Act requires the head of each agency to be responsible for developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of agency information. Outsourcing of IT services, such as network support and website operations, is widespread, and the Department must ensure that contract documents for IT services contain provisions for ensuring that contractors comply with security regulations, guidance, and policy. We found that the Department's information security and acquisition policies contain little guidance for integrating security into acquisitions and that the Federal Acquisition Regulation does not focus on system and data security. As a result, many Commerce contracts contain no provision for security safeguards.

- **Information Security Plan Is Frequently Not Carried Out Throughout the Life Cycle of Agency Systems.** The Security Act requires the head of each agency to ensure that the agency's information security plan is carried out throughout the life cycle of each agency system in order to safeguard the privacy, confidentiality, and security of federal information. The agency head is also to promote security as an integral component of each agency's business operations. As the foregoing discussion has shown, the Department's information security policies need to be updated, oversight needs to be strengthened, and agency managers and program officials need to ensure that effective security policies and procedures are implemented throughout the life cycle of every IT system.

  Information security has yet to become an integral component of the Department's business operations. As a result, fundamental responsibilities are frequently not carried out, including:

  (1) Identifying, assessing, and understanding the risk of the Department's IT assets,
  (2) Determining security needs commensurate with the level of risk,
  (3) Planning, implementing, and testing controls that adequately address the risk,
  (4) Promoting continuing awareness of information security risk and providing appropriate training, and
  (5) Continually monitoring and evaluating policy and control effectiveness of information security practices.

As described previously, the Department is making a concerted effort to improve information security and to make it an integral component of the Department's business operations. The Department's recent actions to improve information security—if accompanied by continued executive-level attention and adequate resources—are important steps in building the foundation for a more effective information security program.